ALETHEO

Aletheo(from Greek - God of Truth) is a framework for text-generation AI with secondary utilities. It allows to transform money into the purest form of power. As it was said in the Bible: “In the beginning was The Word”. The ticker “LET” attempts to highlight the significance of this verse.

Decentralized word-of-mouth marketing service

As of today internet personality bubble reaches absurd levels, a mere mention by an internet celebrity can cost a very significant amount of money. It is generally believed that buying internet personalities' time or creating an ad-trailer should be expensive and it’s worth it, however it appears than a new more effective alternative to this already exists and actively being used. And it is certainly possible to achieve this in a decentralized manner when the employer and the poster don't need to know anything about each other except the stake, eliminating the need of assembling a marketing team or trying to apply to real-life jobs.

What ad trailers and internet personalities attempt to do is not just to sell, but to start a *discussion* to increase awareness, to pump up the popularity of the product. Word-of-mouth marketing, proof-of-discussion, whether it's praising or sick burning, FUD or optimistic insights, blind cult following or elaborate arguments, - the discussion behind the product is what really promotes the product. Celebrities and ads are just a third-party and it is certainly possible to eliminate this third-party and pay directly for discussion and mentions instead. A mass discussion by nobodies for nobodies.

The primary utility of the token is being a sovereign currency for exchange between employers and posters. Employers buy LET token, setup and fund campaigns with that token in LET Market contract with chosen key strings or topics on chosen websites, posters commit to these campaigns by discussing certain posts or anything eligible(matching keyword) for paid discussion. By default, posters are allowed to express any opinion on every topic, and, depending on the resource, posters by default have the right to completely derail the discussion and talk about anything. Posters will get paid for unrelated discussion as long as it for example bumps the thread, or adds another comment to discussion making it look more heated and popular. LET default marketing paradigm promotes critical thinking. Again, it mostly depends on the resource and a forum could simply ban/remove unrelated posts. Posts need to be witnessed by oracles, so a poster has to ensure that his post satisfies the rules of a website. Campaign settings are flexible:

1.Ppp – pay-per-post. Defines how much posters get paid for a post in USD value. As LET token price decreases, the amount of LET being paid to posters increases. USD index is monthly and is average price of LET token last month. Therefore if a campaign lasts more than one month, amount of LET paid per post adjusted automatically to ppp. Ppp can only be increased by the employer if edited.

2.Array of key strings. A key string can be a word or a phrase, a sentence, a text of any length. If employer sets more than one key string, then these key strings become options to make the posting more natural, if a poster mentions just one of those key strings or posts below an op post with one of those key strings, he is eligible for a reward, and there is no point for him to mention all key strings.

3.Mandatory key string can be left blank. Requires to use mandatory key string in every post regardless

whether the post is related to key string discussion or not.

4.Array of target urls. The campaign works only on the websites with these urls. If none set – it means everywhere.

5.minStaked. Minimum requirement of locked LET tokens for a poster to have to join the campaign. It can potentially help with moderation or eliminate the need of moderation completely, depending on the chosen route of marketing campaign.

6.nonEditable, a boolean. Can be set to true in it's inception or at any point in time. If a campaign is non-editable, it can attract funding from other employers, basically allows to make it last longer potentially.

7.noFiring, a boolean. If set to true, posters can't be fired at all, so that posters will more likely join the campaign.

8.onlyManualApproval, a boolean. If set to true, posters can't join the campaign without employer' approval, when this is set, then minStaked is ignored completely, even posters with 0 LET tokens locked can join as long as approved.

9.keyStringPerWords. As an example, in a job which requires 1 key string per 1000 words, if a poster writes 4 posts 250 words each, he has to mention the key string in those 4 posts at least once, and he will get paid for those 4 posts.

10.minPostLength. Minimum amount of symbols in the post to be eligible for a reward.

11.modsPay. Needed if the employer does not feel confident and wants to moderate the campaign, but has no time for that. LET mods are not obliged to follow the rules he wants to enforce, however they are assumed to follow the rules he wants to enforce, since mods salary(independent from modsPay) is not fully tied up to LET to USD index and because the governance can fire them prematurely.

12.rulesLink. A link to a post explaining the rules for posting in detail and ban rules. In the spirit of default LET campaign can be left blank.

13.expirationDate. By default it's 1 month from creation, can be set only longer. If the budget of the campaign is not exhausted, and non-editable set to false, the remaining budget is being refunded to the employer.

14.minCreativity. Minimum poster' sense of humor/creativity which is evaluated by decentralized moderation.

15.postRate. Currently in Polygon blocks. Determines how often a poster can post eligible for payout posts in this particular campaign. Default is ~1 minute, if poster posts more often he is not punished, just not getting paid for more.

16.maxPosters. A limit to make small budgets viable. If not set, might be computed automatically, considering that posters have to cover expenses of rewards claiming.

17.startTime-endTime. By default 0 to 0, which means 24 hours per day. Specifies time of day in GMT timezone, when the campaign is active.

18.An array of campaign languages. Left blank if any language. If not left blank, then only posters who can join are those who stated their language. A poster can't alter his language, he can only choose to set one or not to set at all. From the start, posters of different languages will have same pay-per-post for default campaigns.

On websites which support nicknames posters will eventually be able to talk about anything with nearly anyone anywhere as long as they have keyword in their nicknames.

General philosophy and technical principles

-Politicians are as naive in the face of innovation as we are. All their experience means absolutely nothing when an innovative technology turns upside down everything what they knew about.

-Everything is inefficient. The world scientific progress while advancing everyday is actually close to stagnation in comparison of how fast it could be.

-The probability of a new innovative technology appearing increases exponentially with each passing year. The probability of a new existential threat appearing increases exponentially with each passing year. Humanity either evolves or goes extinct.

-Richest governments spend billions on medical research paying full salaries in their inefficient bloated jurisdictions.

-The world has so much more brain power than ever, and the most of this brain power is unable to innovate.

-Historically most smart people were failing to achieve power, because they were always busy with concepts nobody understands.

-Fundamental value of centralized governance approaches zero. Centralized governance is an existential threat in itself, the very thing it tries to prevent. History has proven it countless times.

-The internet is the watch. The internet saves more lives than all governments' laws combined. As long as we keep open borders for the internet, devastating conventional warfare or even World War 3 won't happen regardless of Power Vacuum.

-Modern humans' views are made of plasticine. They can't even elaborate on their stance about any particular subject, you can change their lives forever with an argument, or simply by rhetorics.

-The audience lacks education. So the internet adapts, dumbs itself down. It's an utter disaster of a civilization, the audience needs to learn how to think. We do not need equality, we need to make humanity Sapiens.

-History shows that privacy of the individual was never respected. We have to demand it as a right, establish it as a right. Empires of the past didn't have the surveillance technology tech giants have today. The upcoming suffocating tyranny of modern tech giants could be multi-millennial.

-Twitter remains centralized text-generation AI' playground for years.

-A department has to deliver the results of their work to superiors even if there is nothing to work on.

-Broken Windows Theory suggests that if there is a window broken in the neighborhood, and for some reason the budget to fix it is lacking, people around become more and more anxious, more subject to anger and poor decision making. It can also be described as Butterfly Effect. Anything that makes our lives more comfortable does exactly the opposite. Any new technology which increases quality of life and any great free software indirectly prevent crime. It positively influences the lives of those who can barely afford any nice things.

-Free software developers are modern Saints. We should fight for them. Supporting free software is supporting Good. We must make these heroes rich.

-Many industries would be thriving with richer high quality free open source availability.

-With increasing complexity of modern software, free open source struggles to keep up with the times, asking for donations is clearly not helping.

-Modern humans are potentially immortal. We don't need a spit in the face in a form of elders' care. We can use our retirement money for cryopreservation.

-Humanity will always remain an existential threat to itself. In the future many absolutely unimaginable technologies will be researched to prevent extinction.

-Dying people just stop wanting to live, because their systems are failing, that's it. That's how we die.

-Eternally healthy humans will strive for new experience and knowledge for eternity.

-LET doesn't care who you are, what's your age, gender, ethnicity or skin color. It's here to preserve the freedom of your opinion.

-Today, cryptocurrency is potentially mutable as is. There are ways to change this.

-Some of the most expensive commercials ever made cost around $30 millions. This amount of money in LET could produce 300 millions of posts, if the compensation is 10 cents per post, and an absolute overkill campaign of 3 billions of posts if the compensation would be set to 1 cent. A campaign of this scale could be used to promote brand commercials on Youtube, build community around official accounts and set given keywords trending for a prolonged period of time on different social networks and potentially create unprecedented so far public interest.

Base contracts

Base contracts will be deployed on Ethereum chain.

https://github.com/SamPorter1984/LET/blob/main/contracts/TrustMinimizedProxy.sol

1.Trust minimized proxy. All contracts except non-upgradeable Founding Event contract will be behind this proxy. It's an altered OpenZeppelin upgradeability contract with some features that allow to remove trust to developers and/or governance. New logic implementation is not being set suddenly, instead it is being stored in NEXT_LOGIC_SLOT up to NEXT_LOGIC_BLOCK_SLOT, or for a month or so. The period allows participants to identify if the deployer or the governance is malicious and therefore to exit safely. Next logic can be canceled in case of a bug discovered or upgraded to after month passes. It is impossible to cancel next logic and immediately propose another next logic, because there is also PROPOSE_BLOCK_SLOT which disallows proposing next logic more often than once a month. It is also possible to add a value to PROPOSE_BLOCK_SLOT if for example a situation arises in which there are no plans to upgrade a particular contract for a time being, so that it keeps participants piece of mind for that period. This variable also can be set to infinity-1 to completely seal the code. As an additional option, there is DEADLINE_SLOT, the block after which it becomes impossible to upgrade the contract at all.

https://github.com/SamPorter1984/LET/blob/main/contracts/VSRERC20.sol

2."Very slow regression ERC-20" implementation(VSR ERC-20). The implementation utilizes standard ERC-20 function _beforeTokenTransfer() in such a way that prevents treasury fund from dumping on the market. The function checks how many blocks passed from rewards genesis block and allows to claim only a certain amount per every passed block. Basically developers and all other participants of LET can only claim rewards within constant emission limits and this hard limit can't be avoided.

Allowances in this ERC-20 implementation are made booleans instead of integers.

bulkTransfer() and bulkTransferFrom() methods require an array of addresses and amounts as arguments and compute balances of an array and only after that compute the balance of msg.sender. BulkTransfer() can be used by treasury to distribute rewards and bulkTransferFrom() will be used by Queue Transfer contract.

https://github.com/SamPorter1984/LET/blob/main/contracts/FoundingEvent.sol

3.Founding Event Contract. This is a non-upgradeable liquidity generation event(LGE) with certain differences. Founders Contract is a trust minimized LGE. It automatically creates liquidity. Nobody can transfer Ether from it. To ensure critically required in case of LET decentralization, the LGE will last for 2 months. Liquidity is not locked at all, instead an incentive to keep liquidity is introduced. Rewards for Founders and liquidity providers in general depend not on the amount of liquidity shares they stake, but on the amount of LET tokens present in their liquidity shares at the time of staking. And this number won't change as long as a given provider does not unstake the tokens. So, for liquidity providers the incentive to provide liquidity and stake increases if the price is going down.

Founders, as well as liquidity providers, are able to switch addresses if they feel the need to, which allows them to claim their stake and rewards from a different address.

Every Ether deposit to Founding Event contract is being subtracted by 1%, and this 1% will be used for audits, bug bounties and development like oracles, servers, RPC, ddos protection, audits and any other expenses required by LET during Founding Event. After that it can be locked as liquidity in trust-minimized cross-chain bridges.

Public temporary database

LET will use fast centralized public blockchains as temporary databases or those optimistic roll-ups which are incapable of censorship. First, LET can probably start from Polygon Network. The database should be blockchain agnostic, because fees on a particular network can become unacceptably high for posters.

Database contract is a simple event emitter with settings variables for oracles to act upon. Posters emit events in database contract with the information about their posts. Oracles then verify if those posts exist. Commit-reveal scheme nearly eliminates front-running as well as disallows oracles to alter the transactions and allows this system to scale to any number of posters and websites.

LET Wallet

LET wallet is a browser extension. The extension fetches specified form data, stores the post and sends a hash of current post and previous post to the blockchain. It can operate on nearly html-js chat. Functionality of this extension is restricted during beta-test to certain imageboards and Twitter by centralized oracle. It will probably be restricted for a lot longer than that, and different relevant websites support will be added gradually over time.

Planned functionality:

1.Custom encoding for languages which could require that, as UTF-8 is inefficient by blockchain standards. Every community dedicated to specific language can submit an efficient encoding scheme if they feel like it's needed. Basically mapping ASCII differently, and every language will require a header stating which language is that.

2.Everything that a modern wallet has, including encrypted keys being stored on the user device only.

3.Limit orders and any other orders useful for dex trading.

4.Queue Transfer contract interface for cheaper but slower transactions.

After extension will be secure enough, the posters will lock a certain amount of tokens in poster wallet to be able to post for campaigns.

Decentralized moderation

Moderators will be elected once a year by the community. First year officials could be elected by Telegram polls, if the governance won't be ready for that. To become a candidate defining language is required and it will be set in stone. To vote for or against candidates, it's also important to define the language(or they can leave it blank, anonymous, except they won't be able to vote for mods and anything else related to specific languages).

Officials are not only mods but also community managers and tech supports, they decide between each other how and what and who will do, and what is required: a blog, a Twitter account, or whatever else.

High value posters will be promoted(given higher pay) by mods, and will be able to help with decentralized moderation as soon as they prove humanness. Posters

who only post meaningless spam will be banned or demoted by the mods. All this will be public and shown on the website with history of addresses they have promoted/banned, so that independent reviewers could point out to unfair moderation and censorship.

Moderators can't ban a poster single-handedly, instead a group of moderators vote, and only most voted addresses are banned.

Moderators will have a base emission of 400 LET tokens yearly and the emission decreases by 25% every 10 million blocks starting from 20 millionth block. The governance will fire lazy or unfair elected officials prematurely. The possibility of having community managers/moderators which hold the position longer than for 1 year is currently being observed.

Tokenomics and Treasury

Token utility and multi-year token locks require high inflation in order to support decentralization progress.

Starting supply: 1 million.

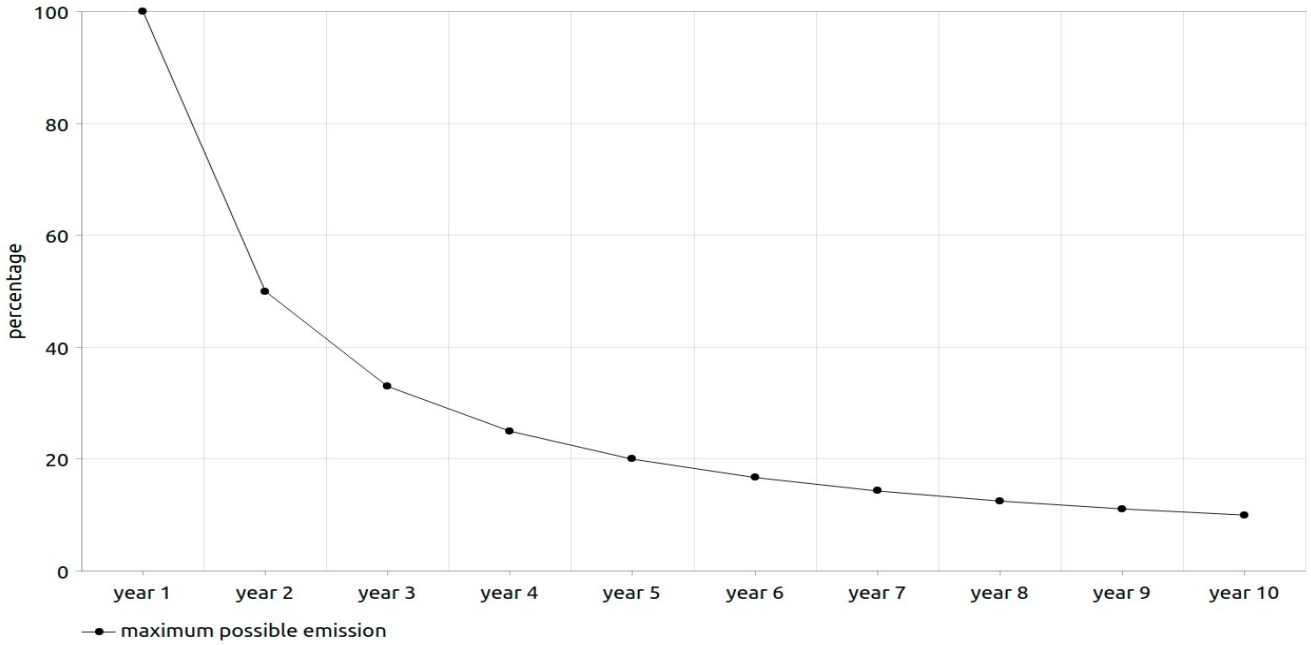
Total supply: 1 billion.

Emission: maximum emission is approximately 1 million each year. Note: while some funds' tokens are being unlocked on fixed schedule, it does not mean that all unlocked tokens are being claimed, so it's better to perceive these numbers as maximum possible inflation, not actual. Treasury will support:

1. Default LET promotion campaigns. Posters will receive salary for default campaigns from treasury. For a prolonged period of time from inception there will be only one default campaign – LET campaign. The formula of rewards for this campaign will not be based on LET to USD monthly index just yet. Instead given poster rewards per period(a period is likely to be 1 month) formula will look like this:

$$rewP = p*tRewP/tP$$

Where p – amount of all witnessed by oracles posts by given poster per this period. tRewP – total rewards for this period for all posters, will be probably fixed and at least account for 40% of all Aletheo emission. tP – total witnessed by oracles posts or all posters during this period.



2. Founders and generic liquidity providers. Founders and liquidity providers have separate rewards pools. Each time when a liquidity pool on a new exchange is introduced, rewards pools with chosen by the governance allocation are being created for this liquidity pool, incentivizing a part of liquidity to migrate to that new liquidity pool.

Rewards for Founders' group will take 20% of maximum possible emission and emission starts when trading goes live on block 12640000(Genesis block). Generic liquidity providers will take another 20% of maximum possible emission. Basically both groups have separate rewards pools.

Starting from block 20 millionth block included, rewards emission decreases by ~25% every 10 million blocks. TokenAmount variable represents the amount of LET tokens in liquidity shares at the time of staking these liquidity shares. Founders' liquidity shares are being staked from the very start, and their total tokenAmount equals to starting supply, 1 million. Generic liquidity providers can only start staking and unstaking after the trading opens.

The formula for founder' tokenAmount in wei for given liquidity pool:

FtokenAmount = pEthC*1e24/tEthC

pEthC – personal Ether contribution to the Founding Event, tEthC – total Ether contributed to the Founding Event.

The formula for a founder' rewards per block in wei for a given liquidity pool:

FRewardsPerBlock = tA*E/tFtA

tA – personal founder' tokenAmount, tFtA – total founders' tokenAmount. Founders can't stake anymore, they can only unstake, thus decreasing tFtA. E stands for emission, starting from 21e16 wei per block on first month.

The formula for a generic liquidity provider' tokenAmount on which rewards per block will be determined:

LPtokenAmount = LPC*tLET/tLPC

LPC – amount of liquidity shares being staked by this liquidity provider at a given time, tLPC – total supply of liquidity shares, excluding founders' liquidity shares, tLET – total amount of tokens present in the pool.

The formula for a generic liquidity provider' rewards per block in wei for given liquidity pool:

LPRewardsPerBlock = tA*E/ttA

tA – personal tokenAmount, ttA – total tokenAmount of all liquidity providers excluding founders. E stands for emission, starting from 21e16 wei per block on first month.

3. Default LET monthly meme NFT contests. Governance will vote for best memes monthly and winning memes are being resubmitted for the next month, therefore best memes can receive rewards for several months.

4. Oracles.

5. Decentralized development of LET network and software, as well as support of established free open-source software. Emission for allocation of every core Aletheo developer is 2k yearly and it decreases by 25% starting from block 20 millionth and every 10 million blocks after that.

LET development starts decentralized from it's inception. At the point of writing this paper 0.5, we have already gathered a team of first main contributors which will have allocations determined by the community: Sam Porter ~32857.142857 LET, Odilitime ~28857.142857 LET, Oro Uma (artist, not developer) – ~19285.714286 LET. All other developers will be hired by the governance, and they will either have a specific fixed allocation or a salary instead based on the monthly index of LET to USD or one time grants for contributions. The treasury can enable developing free open-source alternatives of any closed source proprietary software by hiring a lot of small teams up to 5 people maximum.

6. Non-profit social networks like Mastodon and imageboards. Imageboards require next level popularity, next level mainstream adoption.

7. Anything else that governance will be interested in supporting, as long as functionality for grants and financial support for a particular idea is possible to fulfill in trust minimized way and as long as it is not illegal.

8. Bug bounty and audits.

Pseudo-anonymous oracle network

While LET oracles could provide KYC for simplicity of the design, with Chainlink verifiable random numbers it is possible to allow anonymous and pseudo-anonymous oracles to deliver true results. Oracles shouldn't know what role they are performing in a given iteration of publishing results. There have to be two roles: witnesses and supervisors. Chosen supervisors have to be a small uneven amount of all oracles. Supervisors' results are considered to be true, and witnesses results have to match it. Supervisors have to be a small uneven amount of nodes, 3 out of 20, or 3 out of 100. If supervisors' results don't match, another attempt of choosing supervisors occurs, until supervisors results match, while published results stay, no republishing occurs during that. In case of lies, at least 50% of the stake is burned. Safe limits for inaccuracy which is not considered a lie are yet to be determined. To increase the probability of that the several oracles are definitely not one person, we can use these facts about an anonymous wallet:

1.Balance. Allow anonymous oracles only with considerably high balance. Higher LET balances have the least incentive to lie and ruin posters' trust.

2.Transaction history. Democracy Earth Foundation is building tech which attempts to measure unique humanness. We could use their framework or build our own which evaluates the differences in views in different DAO choices, and not just membership of different DAOs.

LET specifically also can use these variables:

3.Language. Language communities can elect oracles.

4.Poster history activity and uniqueness.

Oracles can at best censor some addresses collectively or approve all existing addresses transactions even if those transactions are fake. If a poster is censored, then he moves to a different oracle cluster, so that censoring oracles lose money, since censorship could be easily verifiable with most resources. In case of fake rewards, the governance will be able to punish oracles, but only within certain limits, depending on the lies occurred. An independent observer software is required for this. This however is still a pending issue to resolve in a trust minimized way. Adopting a supercheap second layer could allow oracles to publish whole threads and thus make everything observable and make lies impossible. Autistic roll-ups could be required for this.

Oracles verify posts and keep the data on the amount of verified posts for every address in their databases and publish the rewards data every month to Polygon chain, so they won't need to keep the data longer than a month. Oracles then use privacy oracle solution like Deco, to generate random disposable keys to move the rewards data from Polygon to Ethereum mainnet through trust minimized cross-chain bridge.

Trust minimized cross-chain bridge

This is the least researched topic in this draft, and should not be considered secure. Commit-reveal scheme disallows oracles to alter transactions. First what he need to do is to announceHash(), Hash has to be generated by the off-chain by the user maybe through a web ui and has to correspond with:

keccak256(abi.encodePacked(userAddress,arg1,arg2,arg3,arg4,anyDisposableKey))

The user keeps all arguments and disposable key to himself, until anonymous trustless oracle network relays the hash to the other chain, he then must verify if the hash is indeed his, and if it is, then he sends the actual transaction with all argument and used disposable key. The contract on the other chain will

only accept address, arguments and a key that matches previously posted hash. If the contract indeed receives correct arguments – oracles are rewarded. This bridge allows not just to cross() or simply relay tokens value, but it also allows to callAcross() - to relay data which enables trustless cross-chain contracts communication. This function will be used by the oracles to relay rewards information from Polygon to Ethereum.

The user can attempt to cancel the transaction even after the hash was relayed, by simply relaying another hash back and withdrawing the funds.

Fundamentally pure governance

If the governance is compromised, it could completely ruin the idea behind the project. Very high minimum quorum and a long period of voting are required. We have to assume that the governance always compromised from the very inception, in that case, we have to make it so that the governance will be unable not to support free software development at all, if it abstains from voting, the grants will be chosen randomly or just about randomly.

Managing treasury requires absolutely next level DAO' purity of intentions. We have to allow only certain options for governance to decide upon fetched by trustless oracle network. Oracles have to fetch only established free open source projects with certain minimum measurable limits like time since inception. Same could go for any other grants governance can approve, oracles can propose only existing established companies or individuals as beneficiaries with verifiable profiles or anyhow transparent and convenient.

A grant is not being transferred in one big transaction. Claiming of the grant as rewards starts from 0, not truly final, and the DAO can revoke it, if something is wrong. Receiving grants address should not be a contract, so it will be much harder for oracles to transparently cooperate for successful lie.

Voting rights are accessible with locking LET tokens for 6 months. Founders and Liquidity providers can also lock their liquidity tokens and vote with their tokenAmount variable. Half of last year of token lock voting is forbidden for a voter, unless he prolongs the lock.

Where it is required, voting can be split in stages: 1.Voting by active human posters without taking into account their stake. 2.Voting by stake.

Beta-test

Beta-test launches together with Founding Event and will last 2 months. During the beta-test, depending on Mumbai testnet capability and if LET and Polygon will be able to reach an agreement, transacting will be free. Only one campaign will be available during beta-test: LET campaign. Posters will be able to claim their beta-test rewards after the Founding Event concludes and trading of LET token goes live. During beta-test posters will be able to specify any secure address to receive beta-test salary, the wallet is not supposed to hold any funds as of yet.

LET chain

While Aletheo protocol will fully function on Ethereum and EVM compatible chains and sidechains, LET chain will be a fork of Oxen and optional to use. Oxen by default is an XMR POS fork, therefore LET chain will have privacy of data by default and it’s smart contracts will be written in HolyC.
If a situation of insufficient decentralization occurs, posters can be allowed to run nodes with virtual stake which can eventually be filled with their salaries to make the chain decentralized in no time. Virtual stake nodes after accumulating at least some balance could help validate 0 value transactions.

If a situation of insufficient adoption occurs which is a security risk, Ethereum Daemon should also exist on the chain

Risks

You acknowledge and agree that investing in cryptocurrency is an extraordinary great risk, there are risks associated with purchasing LET Token or liquidity shares involving LET Token, holding LET Token, and using LET Token or liquidity shares involving LET Token for participation in the LET Network. In the worst scenario, this could lead to the loss of all or part of the LET Token which had been purchased. IF YOU DECIDE TO PURCHASE LET TOKEN, YOU EXPRESSLY ACKNOWLEDGE, ACCEPT AND ASSUME THAT THERE IS NO GUARANTEE OF FINANCIAL RETURN OF ANY KIND AND THAT YOU ARE NOT PURCHASING A SECURITY.
YOU ACKNOWLEDGE THAT ANY LET SOFTWARE WHICH CURRENTLY EXISTS OR MIGHT BE DEVELOPED/ALTERED IN THE FUTURE IS PROVIDED AS IS, WITHOUT WARRANTY OF *ANY* KIND. FINANCIAL RETURNS ARE NOT GUARANTEED AND ALL YOUR MONEY COULD BE LOST.